

## REMARKS

This amendment is responsive to the Office Action of December 14, 2010. That Office Action has been carefully considered but does not address the improper combination that arose from the citation of the inapposite Wiley disclosure after the Zhou disclosure was recognized as not anticipating claims in this application.

Claims 1-12, 14-15 and 17-26 are pending in this application. Claims 1 and 11 have been amended for the sake of clarity. Claims 25-26 have been added to assure that the invention enjoys the full scope of the protection to which it is entitled under the laws of the United States of America. These claims are supported in paragraph [0026] of the specification.

## AMENDMENTS FOR THE SAKE OF CLARITY

The editorial amendment of claims 1 and 11 emphasizes that it is the controller that is in contact with the technician, which is already recited in the preambles of these claims, as well as being supported by paragraphs [0008] and [0024] of the specification.

Specifically, the preambles of claims 1 and 11 recite "providing event-relevant information about an industrial control alarm event occurring in a machine from an industrial controller controlling the machine to a specified remote receiver via a network" [emphasis added]. This is also the purpose of the invention as stated in paragraph [0008]: "It would therefore be desirable and advantageous to provide a simple method for a transmission of messages from industrial controllers to pre-defined receivers or recipients." Paragraph [0024] more specifically discloses that it is "the controller-internal alarm system 2" that is in the controller that generates the "receiver-specific" alarm message that is sent to that specified receiver.

The "specified receiver" that is described in this disclosure and referred to in the claims is the type of recipient for whom conventional security measures, such as PKI encryption are not adequate, as described in paragraph [0007] of applicant's

specification. That “specified receiver” is referred to hereafter as a “roving technician,” which is an example of one type of specified receiver for whom PKI is inadequate -- because they travel from the location of one machine to that of the next rather than having a fixed “office” location.

The “specified receiver” to whom the alarm messages are transmitted in applicant’s disclosure and claims is a mobile receiver that can be used to contact a roving technician, for example using SMS, email, voicemail, etc. -- see paragraphs [0013] – [0014] of applicant’s specification. So long as technicians were located in an office, or at some fixed place, the conventional security methods were usable.

Paragraph [0024] has also been amended for the sake of clarity. No new matter is added thereby. The location of the Web server 4 in the controller 1 in applicant’s disclosed preferred embodiment is supported in Fig. 1 and in the description of the preferred embodiment shown by FIG. 1 that is provided in paragraph [0022] of the specification.

### **USING HINDSIGHT TO COMBINE INAPPOSITE PRIOR ART**

The combination of the Wylie disclosure with Zhou was proposed after the assertion that Zhou anticipated applicant’s claims was withdrawn. However, Wylie is also inapposite, and its proposed combination with Zhou is 1) the product of hindsight. The alarm-event messaging scheme that combination produces is also either 2) centralized and therefore inoperative to solve the problem addressed by the claimed invention, if it were proper to combine the disclosed messaging structures disclosed by Wylie and Zhou, or 3) de-centralized if these disclosures are improperly combined using 1) hindsight, to provide the 3) decentralized alarm event messaging that Zhou teaches away from. Thus, this proposed combination is improper in every respect. This rejection is not supported by the cited art.

### Wylie's Industrial Controllers

Unlike Zhou's multipurpose, centralized ASP, Wylie does disclose industrial machine controllers, special-purpose control computers that are each located with the respective industrial machines that they control, even though some of their I/O modules may not be in the same "rack" as the computer itself, col. 1, lines 44-48. Industrial machine controllers are located with their respective industrial machines because technicians need to use them for on-site maintenance and repair work on those machines, as is well-known in the art. For effective inspection and maintenance of the machines, the operational and alarm event-relevant information that their controllers provide is, necessarily, the most up to date and complete information that can be obtained without taking the machine itself off-line and physically inspecting the condition of the machine's parts in detail, as is well known in the art.

Collocated industrial machine controllers that are similar to those mentioned by Wylie are also disclosed in the German-language disclosures that are of record in this application. While technicians were located at a fixed place, the conventional methods provided by conventional controllers were usable.

### No Security Problems and No Roving Technicians in Wylie

However, the remarkable success of manufacturing-sector exports in the German economy has been made possible by Germany's intensive and ever increasing reliance on industrial automation. That success is reflected in the international balance of payments enjoyed by Germany -- one that is much more favorable than the one achieved by the United States where manufacturing has been on the wane. This economic success has resulted in an ever increasing use of these "roving" technicians in German manufacturing. Each of these roving German technicians is responsible for manufacturing machines at multiple industrial sites and travels between them.

PKI email encryption, and the other conventional measures taken to secure the communications channels used to alert technicians to problems occurring in the machines that they are responsible for are not suitable for use by these roving technicians, as explained in paragraph [0007] of applicant's specification, particularly when the technicians are traveling between these sites. At the same time, the potential costs and liabilities associated with unauthorized access to those machine controllers also increase as Germany's manufacturing plants become more highly automated, as is noted in paragraph [0006] of applicant's specification. It is well known that serious damage can happen very fast in such highly automated plants, regardless of whether the unauthorized act was intentionally malicious or merely incompetent. Therefore, although conventional security measures are too restrictive for use by these roving technicians, who must have alarm messages from and access to their industrial controllers in real time, assuring that only authorized personnel have access to both the alarm event messages and the controllers themselves has also become critically important.

### **1) Zhou is superfluous to Wylie**

Wylie does mention that industrial machine controllers can send alarm event messages to a remote location. The type of conventional controllers described in the German disclosures that are of record in this application also do this. However, none of these disclosures of industrial controllers describes or suggests the problems encountered by Germany's roving technicians when such alarm event messages are sent to their offices by conventional controllers. Thus, none of the art of record discloses or suggests the problem that arose when roving technicians -- who need to receive these alarm event messages in real time while they are traveling if they are to be effective in maintaining safe operation of these manufacturing plants -- found that the conventional security measures such as PKI were not useful to them.

Wylie neither discloses nor suggests that such efficiently deployed, mobile technicians, like those whose roving work assignments support Germany's on-going

economic success, might be advantageous and might need some different security procedures. Instead, Wylie discloses improved diagnostic algorithms for use by the conventional industrial controllers. Wylie is inapposite to applicant's claimed invention.

Since Wylie is inapposite to the problems of these economically important roving technicians, it is not surprising that Wylie's disclosure does not suggest any security problem that would prevent remotely-located technicians from receiving conventional alarm event messages from the conventional industrial machine controllers. On the contrary, Wylie's disclosure suggests that the routine security measures used by conventional industrial machine controllers when sending alarm event messages to remote technicians have been sufficient and satisfactory. In particular, Wylie discloses the use of Internet email as well as other public and private wireless and hardwired communications modalities, without regard for their well-known vulnerabilities. For example, in col. 5, lines 60-65, and col. 8, lines 30-53.

The types of communications that are disclosed by Wylie are not vulnerable when used in the conventional way to contact conventional – non-roving – technicians, by using private networks, and/or encryption methods such as the PKI. However, the while roving technicians are traveling from one controller to another, these non-conventional, roving technicians may only have access to vulnerable public telephone and data networks, and must find some other way to assure that alarm event messages will be displayed on a secure terminal. Alarm event messages sent over public telephone and data networks are vulnerable to misdirection, and/or interception over the public telephone and data networks, but the conventional PKI-encrypted email messages that are conventionally sent to the technician's office, are not reliably accessible outside the technician's office, as was noted in applicant's paragraph [0007].

Since Wylie's disclosure suggests that conventional alarm event messages sent by conventional industrial machine controllers to a remote location are sufficiently secure, Zhou is superfluous to Wylie. The proposed combination with Zhou's disclosure in this Office Action is motivated purely by hindsight, not motivated

by Wylie's disclosure. Therefore this rejection for obviousness over that improper combination of disclosures is erroneous and should be withdrawn.

**2) The One Combination that Can Be Made without Hindsight Is Inapposite**

Conventional alarm event messages can be securely sent by conventional industrial controllers to conventional -- non-roving -- technicians using PKI and private networks, as discussed in paragraph [0007] of applicant's specification. Zhou's system is like Wylie's conventional machine controllers, in that both rely on either the remote ASP or the technician's remote office staff to forward alerts to the roving technician. However, Zhou's system is incompatible with Wylie's conventional machine controllers because Zhou's alarms are generated by the ASP, and even detected at the ASP, unlike applicant's invention.

If Zhou is combined with Wylie, or the other conventional machine controllers, to first securely forward their alarm event messages to a given remote location such as Zhou's ASP and then, secondly, on from there to the roving technicians, those roving technicians eventually will get that message, but that hypothetical combination is also inapposite to the claimed invention, because it is inoperative for improving the communications that the prior art provides for these the roving technicians. Prior art alarm event messaging for these the roving technicians was indirect, inconvenient, and unacceptably delayed. The method provided by that hypothetical combination has the same problems. It does not provide the secure real-time access needed by these technicians.

The result of that hypothetical combination, without hindsight, is that the roving technician's remote office forwards the alarm event message to the roving technician in the field, after the technician's office receives a secure PKI-encrypted alarm-event messages that were sent by the controllers to that office. In contrast, applicant's secure, decentralized alarm event messaging method is advantageous in that it a) eliminates that administrative delay and expense incurred by the prior art.

The method of the present invention is also advantageous for secure communication because it is b) inherently independent of the operational condition of the conventional link between conventional controllers and the technician's fixed centralized office. Therefore applicant's method also provides a direct link to the technician that is a backup for the conventional link between the controller and the office. The method recited in applicant's claims, unlike the inoperative but hindsight-free combination of methods disclosed by Wylie and Zhou, is more reliable, in addition to being more effective, timely, flexible and convenient than the conventional method used by conventional controllers.

This communication system redundancy provided by the direct communication of alarm event messages from the industrial controllers in accordance with applicant's claimed invention -- not disclosed or suggested by either Wiley or Zhou -- is especially important when accident, storm, or flood damages a part of the local communications infrastructure. Zhou's centralized ASP is particularly vulnerable because it needs three links: 1) a data link to sensors, 2) a control link to actuate irrigation valves, etc., and 3) a link to the recipient/receiver, two of which must be continuously available. Even Wylie's conventional industrial controllers require at least two communication links: 1) one from the controller to the office, and 2) another from the office to the roving technician. Applicant's industrial controllers only need one usable link to contact the roving technician. The technician can then either secure that connection, using "https" for example or, alternatively, securely access the controller that sent the alarm event message over any other network that happens to be available and is more convenient for the work that needs to be done. Thus applicant's method secures the communication between the controller and the roving technician and provides flexibility for the technician without sacrificing the critical timeliness and reliability of the technician's access to the controller -- improving both timeliness and reliability relative to conventional controllers' methods.

Using Zhou to communicate between the conventional central office that receives alarm event messages from conventional industrial controllers and the

roving technician, is inoperative to provide the timely, reliable and secure communications needed by roving technicians.

### **3) Zhou Teaches Away from both the Claimed and Hypothetical Methods**

On the other hand, although Zhou's ASP can, hypothetically, be physically combined with the conventional alarm event message communication method used by Wylie's conventional industrial machine controllers, Zhou teaches away from combining that ASP with Wylie's' industrial controllers in this or any other way. Zhou does send alarm event messages from the ASP, and could forward Wylie's conventional alarm event messages from the first, conventional remote location (the technician's office) to a roving technician at a second remote location (traveling in the field). The roving technician would, probably, eventually, get that message, as noted above. However, that combination is inconsistent with the disclosed purpose and advantages of the process used by Zhou's ASP.

On the contrary, Zhou discloses that the remote ASP, which is a multipurpose monitoring and alarm messaging service bureau, is advantageous because it provides monitoring and control functions as well as generating alarm event messages. Zhou's remote ASP is advantageous, and potentially profitable, because it provides all those functions for many different types of events and devices all from at the same centralized location-- see Zhou, paragraph [0005]. That is, the ASP must be 1) non-specialized and 2) provide the control and monitoring functions at the same centralized location that is remote from all of the devices it controls and monitors, and for which it generates alarms. The principal advantage of this centralized, multipurpose, remote ASP is that it provides economies of scale, because it can both control and monitor devices, as well as providing the alarm event messages, all from a single location that is remote from all of them.

Thus Zhou teaches away from both the use of 1) Wylie's industrial controllers that locally monitor and control machines and locally generate alarm event messages that are sent to a central office, and 2) applicant's decentralized communication of



alarm messages from the monitored devices themselves directly to the specified recipients/receivers. Both Wylie and the claimed invention are completely contrary to Zhou's teaching that centralized control and message generation is preferable.

Even without this contrary teaching, combination of Wylie with Zhou would be inapposite because it results in the technician's office contacting the roving technician and not in receiving the message directly from the industrial controller, as noted above. These disclosures not only do not suggest that providing alarm event messages from the controllers to a roving technician would be advantageous, as required for making the combination, Zhou even teaches away from both decentralized control and decentralized alarm message generation. Therefore Zhou cannot possibly suggest a communication method whereby a local, specialized controller directly contacts a specified roving technician.

Zhou, like Wylie, neither discloses nor suggests the security problems of highly automated industrial machines, nor the other problems of providing real time alarms from and access to the industrial machine controllers to the roving technicians who need it. The proposed combination is both internally inconsistent, because it is contrary to Zhou's teaching and the addition of Zhou to Wiley is inoperative to solve the shortcomings of conventional controllers that is addressed by applicant's invention, and changing conventional controllers to transmit alarm messages to roving technicians rather than the roving technicians' fixed offices, is also improperly based on hindsight, not either Wiley nor Zhou. Therefore this rejection should be withdrawn.

#### **REJECTIONS UNDER 35 U.S.C. §103(a)**

Claims 1-4, 7-12, 14-15, and 17-20, have been rejected under 35 U.S.C. §103(a) as obvious over U.S. Patent No. 7,203,560 of Wylie et al., in view of the published U.S. Pat. Appln. No. 2008/0186166 of Zhou et al.

The rejection of these claims under 35 U.S.C. 103(a) is respectfully traversed for the reasons given above.

The rejection of these claims, as amended, under 35 U.S.C. 103(a) is also respectfully traversed.

Specifically, the preamble of applicant's claims 1 and 11 recite a method of "securely providing event-relevant information ... from an industrial controller" and, as amended, those claims now specifically recite "transmitting from the controller to the specified receiver in response to the alarm event a receiver-specific message indicating that the alarm event has occurred". This further emphasizes the controller that is already recited in the elements of these claims, and the communication with the controller that is already recited in their preamble, in particular. No further search is needed.

Zhou cannot be combined with Wylie to forward a controller's message to a roving technician, that is inoperative to solve the problem addressed by applicant's claimed invention and contrary to Zhou's teaching.

Zhou cannot be combined with Wiley to send the controller's message directly to the roving technician. because that combination is a product of hindsight that is not suggested by either disclosure, and it decentralizes both the monitoring/control and the message generation functions, which is wholly contrary to Zhou's teaching.

With particular regard to the rejection of claim 11, as best understood, the rejection seems to suggest that that the "secure connections" disclosed by Wylie and Zhou "include" the modem connection recited in this claim, which would be misleading since conventional controllers communicate with a central office, who can use the conventional alarm messaging, and not a with the roving technician who needs applicant's invention. If that is the basis of the rejection, that rejection is erroneous. However, it seems reasonable to assume that the rejection of claim 11 is actually based on the "same rationale" as that of claim 1. Therefore, it is traversed for the same reason as that given above for the traverse of the rejection of claim 1.

Withdrawal of the rejection of these claims under 35 U.S.C. §103(a) and allowance thereof are thus respectfully requested.

Claim 5 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Wylie in view of Zhou et al., further in view of Qi et al. (US 6892064). This claim depends indirectly from claim 1. Therefore it contains all the limitations thereof and those limitations patentably distinguish this claim over the applied prior art in the same manner as claim 1.

This rejection is therefore hereby respectfully traversed for the reasons given above with respect to the rejection of claim 1 over Wylie and Zhou, et al.

Withdrawal of the rejection of claim 5 under 35 U.S.C. §103(a) and allowance thereof are respectfully requested.

Claim 6 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Wylie in view of Zhou et al., further in view of published U.S. Pat. Appln. No 2007/0208697 of Subramaniam et al. This claim depends directly from claim 1. Therefore it contains all the limitations thereof and those limitations patentably distinguish this claim over the applied prior art in the same manner as claim 1.

This rejection is therefore hereby respectfully traversed for the reasons given above with respect to the rejection of claim 1 over Wylie and Zhou, et al.

Withdrawal of the rejection of claim 6 under 35 U.S.C. §103(a) and allowance thereof are respectfully requested.

## **CONCLUSION**

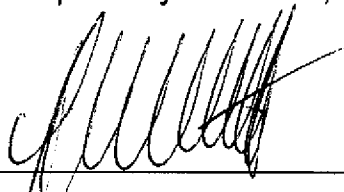
In view of the above, each of the presently pending claims in this application is considered patentably differentiated over the prior art of record and believed to be in immediate conditions for allowance. Reconsideration and allowance of the present application are thus respectfully requested.

Should the Examiner consider necessary or desirable any formal changes anywhere in the specification, claims and/or drawing, then it is respectfully requested that such changes be made by Examiner's Amendment, if the Examiner feels this would facilitate passage of the case to issuance. If the Examiner feels that it might be

helpful in advancing this case by calling the undersigned, applicant would greatly appreciate such a telephone interview.

Respectfully submitted,

By:

  
Henry M. Feiereisen  
Agent For Applicant  
Reg. No: 31,084

Date: March 9, 2011  
708 Third Avenue  
Suite 1501  
New York, N.Y. 10017  
(212) 244-5500  
HMF/RL:be